Bogotá D.C., 17 de noviembre de 2021

Señores
PROVEEDORES
Ciudad

Referencia: CONVOCATORIA PÚBLICA PARA PARA CONTRATAR LOS SERVICIOS PARA LA IMPLEMENTACIÓN, OPERACIÓN Y MONITOREO DE LAS SOLUCIONES QUE CONFORMAN LA ARQUITECTURA DE CIBERSEGURIDAD PARA LA PLATAFORMA TECNOLÓGICA DE LA CÁMARA DE COMERCIO DE BOGOTÁ (CCB), BAJO LA MODALIDAD HÍBRIDA (ON PREMISES Y EN LA NUBE) CON EL OBJETIVO DE PROTEGER LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN EN LA CCB. No. 3000000778.

Asunto: Respuesta a observaciones

Con el presente documento la Cámara de Comercio de Bogotá (CCB) responde a las preguntas allegadas extemporaneamente dentro del proceso de invitación de la referencia.

Pregunta 1
La solución debe implementar protección de vulnerabilidades con nombre (parche virtual) para vulnerabilidades conocidas en el sistema operativo y para aplicaciones que no son del sistema operativo.

Se solicita a la entidad reevaluar esta solicitud dado que este es un punto que cumple solo Kaspersky y trendmicro y en pro de la pluralidad de oferentes y fabricantes participantes en el proceso. Solicitamos sea eliminado o dejarlo como opcional.

Respuesta
Ver respuesta a la pregunta formulada en el literal a de la pregunta 39 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 2
Capacidad de aislar aplicaciones para separar las aplicaciones que no son de confianza del resto del sistema.
Se solicita a la entidad modificar esta solicitud, esto debido a que las soluciones EDR no aislan las aplicaciones, las bloquean , se detienen los procesos o se aisla la máquina.

Respuesta
Ver respuesta a la pregunta formulada en el literal b de la pregunta 39 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 3
El agente de endpoint debe incluir capacidades de engaño (señuelos) basadas en endpoint diseñadas para exponer a un atacante.)
Se solicita a la entidad indicar un poco mas de lo que se espera de la solucion en este requerimiento, un ejemplo de caso de uso de este punto.

Respuesta
Ver respuesta a la pregunta formulada en el literal c de la pregunta 39 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 4
Se debe proporcionar la capacidad de consolidar automáticamente múltiples alertas de múltiples fuentes en un solo incidente.
Se solicita a la entidad también aclarar el throughput requerido en Mbps (Mega bits por segundo) con el fin de estimar el throughput requerido y no solo el consumo total (15 TB)

Respuesta
Ver respuesta a la pregunta formulada en la pregunta 4 del documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 5
Capacidad de cifrado de disco duro.
Se solicita a la entidad eliminar este requerimiento dado que es una capacidad de las soluciones enpoint o productos adicionales y no de un EDR.

Respuesta
Ver respuesta a la pregunta formulada en el literal d de la pregunta 39 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 6
El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB.

Se solicita a la entidad se evalue el requerimiento dado que la informacion que genere el antimalware actual , podria ser utilizada por la solucion del mismo fabricante y se estaria limitando la participacion de mas fabricantes, o poder establecer alguna integración vía api con otro fabrivante según el market place que sea válida.

Respuesta
Ver respuesta a la pregunta formulada en el literal e y f de la pregunta 39 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 7
Monitorear la actividad realizada sobre las aplicaciones y servicios en la nube. En concreto, debe detectar actividad anómala y archivos sospechosos. Debe proporcionar mecanismos que mitiguen las amenazas e impidan la propagación de malware, como entornos sandbox para análisis dinámico o implementando flujos de cuarentena para los ficheros sospechosos.

Se solicita a la entidad, aclara un poco mas el requerimiento, a que caso de uso espeficio se refieren con propagacion de malware ? que caso de uso esperarn cubrir con casb a nivel de propagación.

Respuesta
La solución que presente el proveedor debera cumplir con los requerimientos solicitados

Pregunta 8
Permitir habilitar políticas únicas para dispositivos administrados y no administrados, en navegadores o en aplicaciones móviles enriquecidas.

Se solicita a la entidad indicar a que se refieren con aplicaciones moviles enriquecidas

Respuesta
Ver respuesta a la pregunta formulada en el literal a de la pregunta 40 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 9
Detección multi dimensional de anomalías, con base en Machine learning, que se adapte a los cambios de hábitos de los usuarios.

Se solicita a la entidad que incluya que tambien se puede cubrir este requerimiento , con la deteccion de acciones por monitoreo de actividad , busqueda de malware en apliaciones de storage , reporte y deteccion de cuentas comprometidas o anomalias

Respuesta
Se mantienen los requisitos establecidos en la invitación. El proveedor podrá ofrecer los valores agregados que considere para la prestación del servicio.

Pregunta 10
Detección de ransomware con capacidad de remediar el estado post infección

Se solicita a la entidad revisar la solicitud de este requerimiento, dado que esto esto no aplica para caso de uso en la NUBE es un caso de uso a nivel de endpoint

Respuesta
Ver respuesta a la pregunta formulada en la pregunta 158 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 11
Observaciones generales de CASB
Se solicita a la entidad que puedan incluir en los requerimientos las siguientes funcionabilidades que le permitiran a la entidad contar con una solucion CASB de ultima generacion.
Deberá ser parte del ultimo cuadrante de líderes de Gartner O deberá ser parte del ultimo cuadrante de líderes de IDC Deberá ser parte del ultimo cuadrante de líderes de Forrester
Deberá poder integrarse a una solución de EDR con el fin de otorgar capacidades de XDR
Deberá poder ofrecerse no solo capacidades de SASE sino capacidades de CNAPP
Para los servicios Cloud corporativos como O365, g-suite, Salesforce, servicenow, como mínimo deberán poder ofrecerse coberturas de integración mediante API
Deberán poder ofrecerse reglas de control de acceso para dispositivos administrados y no administrados
Deberá contar con capacidades de UEBA

Respuesta

Ver respuesta a la pregunta formulada en literal b de la pregunta 40 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 12

Observaciones generales de DLP

Se solicita a la entidad que puedan incluir en los requerimientos las siguientes funcionabilidades que le permitiran a la entidad contar con una solucion DLP de ultima generación.
Al no existir actualmente el cuadrante de lideres de gartner para este tipo de soluciones, se deberá presentar al menos el galardón de Gartner como Peer Insights choise en 2020
Deberá otorgar cualidades de clasificación manual?
Ya sea propias del productos o adquiridas de terceros
La solución deberá poder recibir IOC de otras fuentes para determinar no solo si el archivo contiene información sensible, sino si es considerado riesgoso
La consola de administración deberá poder ofrecerse como física, virtual y Saas

Respuesta

Ver respuesta a la pregunta formulada en la pregunta 41 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 13

Numeral 3.3.3 Equipo de trabajo
b) Especialista en la implementación de la solución tecnológica.
"NOTA: Un mismo profesional puede acreditar la experiencia o las certificaciones antes mencionadas, para cumplir con este requisito."

P:// Solicitamos amablemente a la entidad, que la experiencia de los especialistad para la implementación sea presentada en mínimo tres de las soluciones tecnológicas ofertadas. Toda vez que aparte de las soluciones mencionadas en este numeral, es necesario contemplar otras tecnologías adicionales para dar cumplimiento a los requerimientos técnicos contenidos en la presente invitación.

Respuesta

Se mantienen los requerimientos solicitados

Pregunta 14

Al cronograma
Solicitamos amablemente a la entidad, correr la fecha de presentación de la oferta, en por lo menos una semana más, ya que al ser una oferta de complejidad alta, con múltiples soluciones tecnológicas, es necesario contar con un tiempo prudente para organizar la documentación y las ofertas técnias y económicas.

Respuesta

Mediante adenda No.2 se amplió el plazo de cierre.

Pregunta 15

3.2 Modelo de Operación:
El proponente en conjunto con la CCB definirá el mecanismo de registro de los eventos e incidentes de seguridad que se detecten y su gestión.

Agradecemos a la entidad confirmar si se hara uso de la herramienta ITSM de CCB oara el registro de Eventos e incidentes sobre la plataformas de seguridad que se encuentra dentro del alcance de este proceso.

Respuesta

No se debe considerar dentro de la solución propuesta el uso de herramientas internas de la CCB para el registro de eventos e incidentes.

Pregunta 16

3.3 Solución Tecnológica:
La solución tecnológica con la que se prestará el servicio deberá estar aprovisionada en la nube de AWS bajo el modelo de servicio.

Agradecemos a la entidad confirmar si se hara uso de la herramienta ITSM de CCB oara el registro de Eventos e incidentes sobre la plataformas de seguridad que se encuentra dentro del alcance de este proceso.

Respuesta

Ver respuesta a la pregunta 15 de este documento.

Pregunta 17

3.3 Solución Tecnológica:
El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (12) doce meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que los Logs de auditoria de las soluciones propuestas por el Oferente se deben enviar a la solucion SIEM de la entidad para ser almacenados y correlacionados.

Respuesta

El proponenete deberá cumplir con los requerimientos solicitados. La solución deberá estar en el capacidad de enviar los logs a un SIEM cuando la CCB lo requiera.

Pregunta 18

3.3 Solución Tecnológica:
El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por

un tiempo mínimo de (12) doce meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados.

Agradecemos a la entidad confirmar si puede proveer una solucion de Syslog para el almacenamiento de los logs de las plataformas propuesta para este servicio.

Respuesta
Se mantienen los requisitos establecidos en la invitación. El proveedor podrá ofrecer los valores agregados que considere para la prestación del servicio.

Pregunta 19
3.3 Solución Tecnológica:
Soporte con fabricante: los casos o incidentes elevados a los fabricantes de la solución tecnológica propuesta no deberá afectar los acuerdos de niveles de servicio y el alcance de lo contratado.
Agradecemos a la entidad reconsiderar este Item toda vez que dependiendo la criticidad de los incidentes presentados sobre las soluciones a ofertar, los proveedores pueden tomar un mayor tiempo de solucion afectando el cumplimiento de los ANS definidos. En este sentido proponemos que se maneje en la herramienta ITSM un tiempo de escalamiento a proveedor y que este no sea tenido en cuenta en la medicion de los ANS.
Respuesta

Se mantiene los requerimientos solicitados.

Pregunta 20
3.6 Acuerdos de Niveles de Servicio
Tiempo de Solución Máximo: Según complejidad:
▪ Complejidad baja: 60 minutos
▪ Complejidad media: 180 minutos
▪ Complejidad alta: 720 minutos
Al inicio del contrato entre el proveedor y la CCB se definirá los casos específicos a considerar en cada tipo de complejidad.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que los tiempos de solucion deben quedar de la siguiente forma:
▪ Complejidad alta: 60 minutos
▪ Complejidad media: 180 minutos
▪ Complejidad baja: 720 minutos
Respuesta

Se mantiene los requerimientos establecidos en el numeral 3.6 de la invitación a proponer

Pregunta 21
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
La solución debe poder eliminar el malware automáticamente cuando se detecte, es decir, eliminar / poner en cuarentena archivos / matar procesos.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que la solucion que Elimina Malware es el AV de la entidad mas no el EDR. En este sentido agradecemos confirmar si la solucion de EDR debe integrarse con la solucion actual de AV de la entidad.

Respuesta
Ver respuesta a la pregunta formulada en el literal f de la pregunta 39 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 22
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
Todas las capacidades deben entregarse en un solo agente / sensor o integrarse directamente en el sistema operativo.

Agradecemos a le entidad confirmar si la solucion propuesta ´puede ser desplegada en varios agentes.

Respuesta
El proponente debe definir la solución tecnológica que cubra lo solicitado en el apartado "Requerimientos Técnicos"

Pregunta 23
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
• La solución debe implementar protección de vulnerabilidades con nombre (parche virtual) para vulnerabilidades conocidas en el sistema operativo y para aplicaciones que no son del sistema operativo.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que la solucion de EDR debe poder realizar parchado virtual en estaciones de trabajo y servidores.

Respuesta

La solución debe implementar protección de vulnerabilidades para vulnerabilidades conocidas en el sistema operativo y para aplicaciones que no son del sistema operativo.

Pregunta 24
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
• Debe incluir el acceso a sandbox en la nube.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que el servicio EDR debe incluirse con opcion de Sandboxing para la explotacion de malware.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados

Pregunta 25
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
El agente de endpoint debe incluir capacidades de engaño (señuelos) basadas en endpoint diseñadas para exponer a un atacante.

Agradecemos a la entidad aclarar este item toda vez que la funcionalidad solicitada hace parte de una solucion de Deception y no una funcionalidad a nivel de Endpoint.
Respuesta

Ver respuesta de la pregunta 146 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 26
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
Capacidad de cifrado de disco duro.

Agradecemos a la entidad reconsiderar este Item y considerar queel cifrado de disco se realice desde el SO a traves de la funcionalidad de Bitlocker

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados

Pregunta 27
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB.

Agradecemos a la entidad confirmar la marca de la solucion Antivirus que actualmente tiene la Entidad.
Respuesta

Ver respuesta a la pregunta 21 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 28
3.8 Requerimientos Técnicos: Endpoint Detection and Response (EDR):
El agente de endpoint debe incluir capacidades de engaño (señuelos) basadas en endpoint diseñadas para exponer a un atacante.

Agradecemos a la entidad reconsiderar este item toda vez que esta funcionalidad limita las soluciones que el Oferente puede presentar para el cumplimiento de esta oblicacion.
Respuesta

La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados

Pregunta 29
3.8 Requerimientos Técnicos: Data Loss Prevention (DLP):
Debe incorporar técnicas avanzadas de inspección de contenido para identificar contenido complejo y aplicar medidas correctivas.

Agradecemos a la entidad aclarar nuestro entendimiento cuando se menciona a contenido complejo.
Respuesta

La solución deberá inspeccionar contenido que puede ser palabras o expresiones.

Pregunta 30
3.8 Requerimientos Técnicos: Data Loss Prevention (DLP):
Usuarios:
Agradecemos a la entidad confirmar la cantidad de usuarios que requieren el servicio de DLP
Respuesta

Ver respuesta de la pregunta 114 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 31
3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.

Solicitamos amablemente a la entidad indicar cuales son los puertos http utilizados por las 50 aplicaciones web.
Respuesta

Esta información será compartida con el proveedor seleccionado
Pregunta 32
3.8 Requerimientos técnicos Web Application Firewalls (WAF)
El Firewall de Nueva Generación y el Firewall de aplicaciones web para AWS deben integrarse de forma nativa para realizar cuarentena de direcciones IPs y de esta forma proteger el tráfico dirigido hacia las aplicaciones web.

Solicitamos amablemente a la entidad aclarar el tipo de integración requerida entre el FaaS y WAF.
Respuesta

La solución deberá integrar de manera Nativa con el fin de que las políticas funcionen en los dos FW

Pregunta 33
3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.
Solicitamos amablemente a la entidad aclarar nuestros entendimiento si las 50 aplicaciones web corresponden a 50 dominios.
Respuesta

Esta información será entregada al proveedor seleccionado

Pregunta 34
3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.

Solicitamos amablemente a la entidad y de ser posible la entrega de una arquitectura / topología de como están dispuestas las aplicaciones web en AWS para poder dimensionar más precisamente la solución.
Respuesta

Ver respuesta a la pregunta 8 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 35

3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.

Agradecemos a la entidad confirmar si las aplicaciones WEB a proteger se encuentran publicadas en internet.

Respuesta

Ver respuesta a la pregunta 7 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 36

3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que este componente se puede ofrecer en SaaS toda vez que las caracteristicas solicitadas se pueden ofrecer desde este componente.

Respuesta

La solución tecnológica propuesta debe ser bajo modelo SaaS.

Pregunta 37

3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.

Agradecemos a la entidad confirmar cuantos y cuales son los dominios de las 50 aplicaciones.

Respuesta

Esta información será entregada al proveedor seleccionado

Pregunta 38

3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.

Agradecemos a la entidad confirmar el Trafico consumido por cada una de las 50 aplicaciones que requieren protección.

Respuesta

Ver respuesta a la pregunta 4 de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 39

3.8 Requerimientos técnicos Web Application Firewalls (WAF)
Aplicaciones WEB a proteger: hasta 50.

Agradecemos a la entidad confirmar si la solucion inspeccionara trafico adicional (TCP y/o UDP) al HTTP y/o HTTPS.
Respuesta

Se debe inspeccionar todo trafico solicitado ya sea TCP o UDP, así como trafico web http / https, y servicios tipo API (https).

Pregunta 40
3.8 Requerimientos técnicos Firewall como servicio (FWasS):
Solución de protección de redes con características de Next Generation Firewall (NGFW) virtualizado para la seguridad de la red empresarial. El fabricante debe pertenecer al cuadrante mágico de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales":

Agradecemos a la entidad confirmar la la tasa de sesiones concurrentes por segundo estimadas para este Firewall.
Respuesta

Ver respuesta a la pregunta 51 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 41
3.8 Requerimientos técnicos Firewall como servicio (FWasS):
Solución de protección de redes con características de Next Generation Firewall (NGFW) virtualizado para la seguridad de la red empresarial. El fabricante debe pertenecer al cuadrante mágico de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales":

Agradecemos a la entidad confirmar la la tasa de log rate por segundo estimadas para este Firewall
Respuesta

Esta información será compartida con el proveedor seleccionado

Pregunta 42
3.8 Requerimientos técnicos Firewall como servicio (FWasS):
Solución de protección de redes con características de Next Generation Firewall (NGFW) virtualizado para la seguridad de la red empresarial. El fabricante debe pertenecer al cuadrante mágico de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales":

Agradecemos a la entidad confirmar las funcionalidades requeridad por el FWaaS.
Respuesta

La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados

Pregunta 43
3.8 Requerimientos técnicos Firewall como servicio (FWasS):
Solución de protección de redes con características de Next Generation Firewall (NGFW) virtualizado para la seguridad de la red empresarial. El fabricante debe pertenecer al cuadrante mágico de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales":

Agradecemos a la entidad confirmar si es necesarioa la retención (en días) de logs para la solucion de FWaaS. En caso de ser afirmativa la pregunta Indcar los periodos de retencion requeridos.
Respuesta

Ver numeral 3.3 de invitación a proponer

Pregunta 44
3.8 Requerimientos técnicos Firewall como servicio (FWasS):
Solución de protección de redes con características de Next Generation Firewall (NGFW) virtualizado para la seguridad de la red empresarial. El fabricante debe pertenecer al cuadrante mágico de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales”:

Agradecemos a la entidad confirmar que tipo de aplicaciones deben ser protegidas por el FWaaS
Respuesta

Esta información será entregada al proveedor seleccionado.

Pregunta 45
3.8 Requerimientos técnicos Firewall como servicio (FWasS):
Solución de protección de redes con características de Next Generation Firewall (NGFW) virtualizado para la seguridad de la red empresarial. El fabricante debe pertenecer al cuadrante mágico de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales”:

Agradecemos a la entidad confirmar el Througput o trafico esperado que debe pasar por el FWaaS.
Respuesta

Ver respuesta de la pregunta 4 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 46
3.8 Requerimientos Técnicos: Autenticación de Usuarios:
Cantidad de usuarios: 2200
'Agradecemos a la entidad confirmar:
o De los 2.000 usuarios, ¿Cuántos son internos, externos/colaboradores, o de otros tipos?
Respuesta

Esta información será compartida con el proveedor seleccionado

Pregunta 47
3.8 Requerimientos Técnicos: Autenticación de Usuarios:
Autenticar tanto a los usuarios como a las máquinas, incluyendo el escenario en donde los colaboradores traen sus propios dispositivos personales a la red empresarial.

'Agradecemos a la entidad confirmar:
'- ¿Qué se refieren con “Autenticar tanto a los usuarios como a las maquinas, incluyendo el escenario donde los colaboradores traen sus propios dispositivos personales a la red empresarial”?

Respuesta: Ver respuesta de la pregunta 133 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

- ¿Cómo se realiza a día de hoy? ¿Cómo se espera que les demos una solución? (Autenticación mediante tarjeta o clave inteligente?
- ***Respuesta*** *esta información será entregada al proveedor seleccionado*

Pregunta 48

3.8 Requerimientos Técnicos: Autenticación de Usuarios:
Integrarse con el Directorio Activo de la CCB.

Agradecemos a la entidad confirmar:
o¿Solo se plantea integrar el Directorio activo de la CCB? ¿Cuentan con multidominio? Si es así, necesitamos la topología de AD.
Respuesta
Ver respuesta de la pregunta 137 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021. El resto de la información será entregada al proveedor seleccionado.

Pregunta 49

3.8 Requerimientos Técnicos: Autenticación de Usuarios:
Integrarse con el Directorio Activo de la CCB.

Agradecemos a la entidad confirmar:
o ¿La solución puede ser 100% cloud?. **Respuesta**: El servicio es Modelo SaaS para todos sus entregables y la solución tecnológica debe estar aprovisionada en nube.
o ¿Cuándo entornos se necesitan montar? (DEV/PRO). ***Respuesta****: Esta información será entregada al proveedor seleccionado*

Pregunta 50

3.3.2. EXPERIENCIA DEL PROPONENTE
contratos ejecutados y/o en ejecución a partir del 1 de enero de 2018

Se solicita por favor permitir acreditar servicios con ejecución desde el 1 de enero de 2015 independientemente de la fecha de inicio del contrato toda vez que, consideramos, lo pertinente es acreditar servicios prestados en los últimos años sin que necesariamente sean contratos iniciados recientemente.
Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 51

3.3.2. EXPERIENCIA DEL PROPONENTE
...constar la ejecución de las siguientes actividades
Considerando que los servicios requeridos contienen actividades que podrían ser mencionadas de manera diferente por cada contratante pero que su alcance es el mismo, se solicita por favor permitir presentar certificados de contratos que incluyan servicios con actividades similares en su alcance pero que el nombre de éstas no sea excluyente o inhabilitante.
Respuesta

En las certificaciones presentadas debe constar como mínimo la prestación de servicios de ciberseguridad para plataformas tecnológicas en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información, por consiguiente, si los servicios que se presenetan en la certificación cumplen con la acreditación de la experiencia solicitada se tendrán en cuenta, sin embargo, será responsabilidad del equipo evaluador valorar cada una de las certificaciones aportadas por el proponente.

Pregunta 52

3.3.2. EXPERIENCIA DEL PROPONENTE
...indicar el monto ejecutado del contrato antes de IVA a octubre

Teniendo en cuenta que la fecha de cierre del presente proceso es a futuro y que los contratantes no podría acreditar valores ejecutados a futuro; se solicita por favor permitir presentar certificados que acrediten valores contratados toda vez que la información de los mismos podrá ser verificada por la CCB.

Respuesta

No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 53

6.3 SEGUNDA FASE DE EVALUACION DE LAS OFERTAS: Calificación
Precio
Para la Segunda Fase de Evaluación de las Ofertas que corresponde a la calificación de las mismas se dispone unos criterios para la asignación de puntajes donde uno de ellos es el menor valor; teniendo en cuenta la facultad de la CCB para llamar a una negociación según lo dispone el numeral 1.14, por favor indicar la forma en que se dará a conocer a los proponentes el resultado de su calificación y la forma en que será posible realizar observaciones a las propuestas competidoras.

Respuesta

Como se indica en el citado numeral, en caso en que la CCB decida realizar la etapa de negociación, informará a los proponentes el procedimiento establecido para tal fin. Por consiguiente, de llegarse a presentar la etapa de negociación se informará por correo electrónico a el proponente con mayor puntaje o a los proponentes que hayan cumplido los requisitos mínimos habilitantes exigidos en la presente invitación, o a los proponentes empatados, para que presenten una contraoferta en relación a la oferta inicialmente presentada. Las propuestas de los demás proponentes no se darán a conocer.

Pregunta 54

6.3 SEGUNDA FASE DE EVALUACION DE LAS OFERTAS: Calificación
El proponente que este inscrito, certifique o cuente con algún sello sobre trabajo en programas y/o aportes a la sostenibilidad (medio ambiente o impacto social enmarcados en los ODS de las Naciones Unidas) de un tercero idóneo como Pacto Global, ICONTEC con su sello de sostenibilidad, Estándares GRI o Sistema B, o podrá obtener el puntaje, el proponente que acredite su condición como Sociedad Comercial de Beneficio e Interés Colectivo, o Sociedades BIC. Calidad que se verificará en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio correspondiente, obtendrá 1 punto.

Aporte a la sostenibilidad… De auerdo a las condiciones establecidas, entendemos que para obtener el punto de calificación se podrá presentar el certificado ISO14001 vigente. Por favor indicar si nuestro entendimiento es correcto.

Respuesta

Su entendimiento es correcto.

Pregunta 55

3.3.3. EQUIPO DE TRABAJO

El proponente debe ofrecer un equipo de trabajo conformado como se describe a continuación, para lo cual deberá presentar las hojas de vida y las certificaciones de experiencia y formación del personal que dispondrá para la CCB.

Considerando que los proponentes plantean una oferta manifestando la capacidad de contar con los profesionales para ejecutar el servicio sin la necesidad de tener compromisos precontractuales laborales en etapa de oferta y con miras a posibles adjudicaciones, que la presentación de hojas de vida no debería ser vinculante dado que entre adjudicación e inicio del contrato se pueden presentar cambios en el personal propuesto por decisiones propias de los profesionales y que el proponente puede presentar un esquema de roles y perfiles con el cual se comprometa toda vez que no es posible asegurar recursos específicos asociados a una operación que aún no ha sido adjudicada; agradecemos a la entidad el solicitar la presentación de las hojas de vida previo a la firma del acta de inicio del contrato.

Respuesta

No se acepta su observación, el equipo de trabajo es un requisito habilitante, razón por la cual se solicitan las hojas de vida y la firma de la carta de compromiso. Se mantienen los requisitos solicitados.

Pregunta 56

5.2. FORMA DE PAGO.

La CCB pagará al CONTRATISTA de manera mensual el valor del contrato por los servicio efectivamente prestados previo recibo a satisfacción por parte del Supervisor del contrato y de los entregables.

Se solicita respetuosamente a CCB fijar un plazo para emitir el recibo a satisfacción de los mismos.

Respuesta

No se acepta su observación.

Pregunta 57

6) OBLIGACIONES DEL CONTRATISTA:

l) Responder ante LA CÁMARA y ante terceros por todas las fallas, errores y omisiones que se presenten en la ejecución del presente contrato y por los perjuicios que con ello se generen.

Se solicita respetuosamente a CCB modificar e incluir a la redacción de este númeral: "por fallas, errores y omisiones imputables exclusivamente al Contratista"

Respuesta

En el caso en que su empresa sea la adjudicataria, se incluirá lo propuesto por ustedes.

Pregunta 58

24) CONFIDENCIALIDAD

"...Esta obligación se mantendrá por término indefinido, aún después de terminada la relación que llegue a vincular o no formalmente a las partes…"

Se solicita respetuosamente a CCB limitra el termino de cofidencialidad, proponemos que sea de 5 años, una vez terminada la relación de contractual.

Respuesta

En el caso en que su empresa sea la adjudicataria, se incluirá lo propuesto por ustedes.

Pregunta 59

32) CLÁUSULA DE APREMIO.

En el caso de mora o simple retardo en el cumplimiento de las obligaciones estipuladas en el contrato dentro del plazo, o en la comunicación expresa en la cual se indique el término en el que deban cumplirse cualquiera de las obligaciones establecidas en el presente contrato, o el incumplimiento de la obligaciones pactadas o cumplimiento imperfecto o defectuoso de las mismas, EL CONTRATISTA pagará a LA CÁMARA, a título de penalidad de apremio, por cada día de mora o retardo, el equivalente al 0,1% del valor total estimado del contrato sin que supere el diez por ciento (10%) del valor del mismo, por cada evento.

Se solicita respetuosamente a la CCB eliminar esta clausula en la medida que su aplicación es diaria, y es en relación con cada incumplimiento, lo que puede resultar bastante gravoso para el contratista, y la idea es conminar al cumplimiento y no poner al contratista en una situación de déficit. Igualmente se tiene la penalización anticipada de la cláusula penal, descuentos por incumplimientos de las ANS por lo que podría presentarse la aplicación de una doble sanción por un mismo hecho.

Respuesta

No se acepta su observación. Lo anterior, con el fin de salvaguardar los recursos de la CCB.

Pregunta 60

PARÁGRAFO TERCERO: EFECTOS DE LA TERMINACIÓN.

La CAMARA se reserva el derecho de exigir la indemnización de los perjuicios causados por alguna de las causales de terminación indicadas en esta cláusula, salvo si el contrato termina por mutuo acuerdo en el que expresamente se pacte que no se pagará indemnización de perjuicios alguna o por el agotamiento de su objeto.

Se solicita respetuosanete a la CCB limitar la idemnización de perjuicios mediante la siguiente redacción sugerida donde se resalta la expresión a incluir: "La CAMARA se reserva el derecho de exigir la indemnización de los perjuicios causados por alguna de las causales de terminación indicadas en esta cláusula, los cuales no serán mayor al valor del contrato, salvo si el contrato termina por mutuo acuerdo en el que expresamente se pacte que no se pagará indemnización de perjuicios alguna o por el agotamiento de su objeto".

Respuesta

No se acepta su observación.

Pregunta 61

La solución tecnológica con la que se prestará el servicio deberá estar aprovisionada en a nube de AWS bajo el modelo del servicio.

Observación: No es claro ese modelo como servicio en AWS, si se instalará en la nube de AWS de CCB o en la nube de AWS del proponente.

Respuesta

Ver respuesta a la pregunta 3 en el documento de Observaciones Invitación Pública 3000000778 fechado 10 de noviembre de 2021

Pregunta 62

El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (12) doce meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados.

Observación: No está claro si ese espacio de almacenamiento de logs debe realizarse en cada una de las herramientas a ofertar o en un SYSLOG/SIEM a emplear.

Respuesta

Ver respuesta a pregunta 17 de este documento.

Pregunta 63

El fabricante debe pertecener al cuadrante mágico de Gartner para plataformas de protección de endpoints.

Observación: De manera atenta quisiéramos solicitar a la CCB evaluat la osibilidad de permitir la oferta de la solución Cortex XDR entendiendo los siguientes argumentos:

1. Cortex XDR no fue incluido en esta ocasión por Gartner debido un tecnicismo porque no cumplió con la cantidad de endpoints instalados. Esto se debe a que el producto estuvo en procesi de re branding (Traps a Cortex xdr), entendimiento que el producto si cumplía con este requerimiento con la marca previa “Traps”. Ver documento de Gartner al respecto:
2. Hoy en día Cortex XDR cuenta con una calificación de 4.6 en el gartner peer insights.

Respuesta

Se mantienen los requerimientos solicitados.

Pregunta 64

La solución debe implementar protección de vulnerabilidades con nombre 8parche virtual) para vulnerabilidades conocidas en el sistema operativo y para aplicaciones que no son del sistema operativo.

Observación: De manera atenta y con fines de permitir la pluraliad de oferente quisiéramos solicitar a la CCB evaluar la posibilidad de permitir la oferta de soluciones que no cuenten con esta funcionalidad. Fabricantes como Sophos, mcafee entre otros no cuentan co la funcionalidad.

Respuesta

Se mantienen los requerimientos solicitados.

Pregunta 65

Plataforma de logs y reportes con capacidad de retención hasta 1 año.

Observación: Es posible llevar los logs vía syslog a un repo externo?.

Respuesta

Ver respuesta a la pregunta 17 de este documento.

Pregunta 66

El fabricante debe pertenecer al Cuadrante máico para firewalls de aplicaciones web de Gartner,

Observación: De manera atenta y entendiendo que la CCB esta volcada a infraestructura basada en micro servicios, quiseramos solicitar a la CCB evaluar la posibilidad de permitir la oferta de soluciones que se acoplen a este modelo, lo cual se difiere de los WAF tradicionales basados en proxy reverso. Adicionalmente, Gartner no cuenta con un cuadrante mágico para este tipo de soluciones debido a que son my nuevas en el mercado y la implementación de una solución WAF tradicional tarerá complicaciones en la operación de la CCB, debido a la complejidad.
Respuesta

Se mantienen los requerimientos solicitados

Pregunta 67
Aplicación WEB a proteger: hasta 50
Pregunta: De manera atenta quisiéramos preguntar a la CCB sies posible darnos información adicional de los servicios asociados a estos sitios web (cantidad de EC2, cantidades containers (nodos), si usan FaaS, etc...) para fines de un correcto dimensionamiento.

Respuesta*: Esta información será entregada al proveedor seleccionado.*

Atentamente,

Cámara de Comercio de Bogotá
[Fin del documento]